Brustoloni 6-3

Abstract of the Disclosure

Clients that are connected on a private network and which are assigned a private IP address that is not routable on the Internet can connect to the Internet through a router/server that includes a network address translator (NAT). For

5 outgoing packets, the NAT translates the client's private source IP address and generalized port number (GPN) to the NAT's global IP address and GPN. For incoming packets sent to the NAT's global IP address and GPN, the NAT translates the global destination IP address and GPN to the client's private IP address and GPN. For protocols which cannot be directly supported by the NAT, such as those

10 in the IPSec security protocol suite, the NAT is extended by creating in the NAT's translation table an entry that associates, for a specific unsupported protocol, a client's private IP address and GPN, the NAT's global IP address and GPN, and a foreign address on the Internet, that is valid until a specified or default expiration time. Outgoing packets from the client to that foreign address and incoming packets

15 from that foreign address to the NAT's global IP address and GPN are translated according to the entry until the entry expires. In associations with these translations to outgoing and incoming packets, the client implements any Application Layer Gateway (ALG) that would otherwise be implemented at the NAT. Further, at the client, outgoing packets are modified before being transmitted so as to pre-

20 compensate for the effects of the translations. Incoming packets at the client from the NAT are similarly modified so as to post-compensate for the effects of the translations. For the IPSec protocol, these modification include adjusting the checksum in the TCP or UDP header to account for IP address and TCP or UDP port number translations.